Computer system operating method for military vehicle or aircraft

Patent number:	DE19618105
Publication date:	1997-11-13
Inventor:	SCHMIDT DIRK DR (DE); GREIN NICOLAS (DE)
Applicant:	PIETZSCH IBP GMBH (DE)
Classification:	
- international:	***G06F11/20; G06F15/16;*** **G06F11/20; G06F15/16;** (IPC1-7): G06F11/20; G06F11/30; G06F15/173
- european:	G06F11/20F; G06F15/16D
Application number:	DE19961018105 19960506
Priority number(s):	DE19961018105 19960506

Abstract of **DE19618105**

The computer system operating method has computer units (1-3) interconnected via a data bus (4-6) and on which each computer unit has one store (31,32). One copy of the software program running on each computer unit (1-3) is stored, with the status of the given software program cyclically transferred from each computer unit (1-3) to the other computer units. The received status is stored (1-3) and the relevant software program started, if a disruption occurs in one computer unit (3), on another computer unit (2), or distributed on to several other computer units (1,2), with the last stored status utilised.

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 196 18 105 A 1**

(51) Int. Cl.[6]:
G 06 F 11/20
G 06 F 11/30
G 06 F 15/173

(21) Aktenzeichen: 196 18 105.4
(22) Anmeldetag: 6. 5. 96
(43) Offenlegungstag: 13. 11. 97

(71) Anmelder:
IBP Pietzsch GmbH, 76275 Ettlingen, DE

(74) Vertreter:
BOEHMERT & BOEHMERT, 80801 München

(72) Erfinder:
Schmidt, Dirk, Dr., 76297 Stutensee, DE; Grein, Nicolas, 76870 Kandel, DE

(56) Entgegenhaltungen:
US 43 56 546
KOBUS, S. und andere: Grundzüge der Zentralsteuerung für das Vermittlungssystem Metacouta L, in: Elektrisches Nachrichtenwesen, Bd. 47, No. 3, 1972, S. 157-161;

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Rechnersystem und Verfahren zum Betreiben eines Rechnersystems

(57) Die Erfindung schlägt ein Verfahren zum Betreiben eines Rechnersystems vor, welches aus wenigstens zwei Rechnereinheiten besteht, die über einen Datenbus miteinander verbunden sind. Jeder Rechner hat einen Speicher und eine Schnittstelle zu dem Datenbus. Gemäß dem hier offenbarten Verfahren wird eine Kopie der Programme, die auf jeder Recheneinheit laufen, in den Speichern der jeweils anderen Recheneinheiten gespeichert. Der Status der laufenden Programme wird zyklisch über den Datenbus von jeder Recheneinheit zu den jeweils anderen Recheneinheiten übertragen und dort gespeichert. Wenn eine Recheneinheit gestört ist, wird eine Kopie der entsprechenden Software-Programme auf einer anderen Recheneinheit unter Verwendung des zuletzt gespeicherten Status gestartet. Gemäß einer vorteilhaften Ausführungsform ist jede Recheneinheit über ein Peripheriebus mit Peripheriegeräten verbunden. Die Peripheriebusse der einzelnen Rechnereinheiten sind über gesteuerte Schalter miteinander verbindbar, so daß bei Störung einer Recheneinheit deren Peripheriebus mit dem Peripheriebus der anderen Rechnereinheit verbunden werden kann, auf der die Software-Programme der gestörten Rechnereinheit gestartet wird.

DE 196 18 105 A 1

DE 196 18 105 A 1

Beschreibung

Die Erfindung betrifft ein Rechnersystem und ein Verfahren zum Betreiben eines Rechnersystems, insbesondere eines Rechnersystems für Landfahrzeuge, welches mehrere redundante Komponenten aufweist.

In zivilen und militärischen Anwendungen, z. B. in der Flugtechnik, bei militärischen Landfahrzeugen, in Kernkraftwerken usw., spielt der Einsatz von elektronischen Komponenten und Computern zur Unterstützung der Bedienung und Steuerung durch den Menschen und zur Steigerung der Leistungsfähigkeit eine immer größere Rolle.

Im Zuge der Automatisierung von Routine- und Steuerungsaufgaben sowie der Verringerung der Arbeitskräfte werden traditionelle Aufgaben des Menschen zunehmend von Rechnern und daran angeschlossenen Peripheriegeräten unterstützt bzw. übernommen. Insbesondere bei so kritischen Anwendungen, wie den oben genannten, erfordern das Umfeld, in dem die Rechner arbeiten, sowie die Sicherheitsanforderungen eine maximale Zuverlässigkeit, die in der Regel durch geeignete Redundanzmechanismen erreicht werden kann. Andererseits verbieten es straffe Kostenvorgaben im Verteidigungs- wie im Zivilbereich häufig, technisch aufwendige Lösungen, wie die Mehrfachauslegung von Systemen, zur Erhöhung der Zuverlässigkeit einzusetzen.

Für den Einsatz von Rechnern in sicherheitskritischen Bereichen, wie der Avionik oder der Kernkraftwerkstechnik, sind Systeme bekannt, mit denen eine Redundanz und Auswahlsicherheit von Rechnern bzw. Rechnerverbunden erreicht wird. Bei diesen Systemen werden sicherheitskritische Baugruppen, zu denen gerade die Rechner selbst gehören, mehrfach ausgelegt. Wenn der Ausfall einer Baugruppe erkannt wird, bewirkt ein geeigneter Steuermechanismus, daß eine zusätzliche Ersatzbaugruppe die Aufgabe der ausgefallenen Baugruppe übernimmt. Diese Ersatzbaugruppe wird nur für den Zweck der Redundanz bereitgehalten und ist normalerweise nicht aktiviert. Durch diese Mehrfachauslegung der Systeme entstehen jedoch sehr hohe Kosten. Die mehrfach bereitgestellte Hardware, die im ungestörten Betrieb nicht genutzt wird, stellt ferner eine große Resourcenverschwendung dar.

Es ist somit eine Aufgabe der vorliegenden Erfindung, ein Rechnersystem und ein Verfahren zum Betreiben des Rechnersystems anzugeben, die insbesondere für sicherheitskritische Anwendungen eine zufriedenstellende Ausfallsicherheit gewährleisten, ohne zu einem erheblichen Mehraufwand an Hardware und somit Kosten zu führen.

Diese Aufgabe wird durch ein Verfahren nach Anspruch 1 und ein Rechnersystem nach Anspruch 9 gelöst.

Die Erfindung sieht ein redundantes Rechnersystem vor, das aus mehreren Rechnereinheiten besteht, die über schnelle Datenverbindungsbusse miteinander verbunden sind. Die Software-Programme, welche auf den jeweiligen Rechnereinheiten laufen, sind in einem Massenspeicher oder in einem Arbeitsspeicher jeweils jeder Rechnereinheit gespeichert. Bei Ausfall einer Rechnereinheit bzw. eines Rechners kann dessen Aufgabe vollständig von anderen, im System vorhandenen Rechnern übernommen werden. Hierfür werden die Programme des ausgefallenen Rechners entweder insgesamt in einem anderen Rechner des Systems gestartet, oder sie werden auf mehrere Rechner in dem System verteilt. Zu

einem gegebenen Zeitpunkt ist dabei jeweils nur eine Version eines Anwendungsprogramms in einer Rechnereinheit aktiv.

Während des Betriebs wird zyklisch der Status, z. B. in der Software vereinbarte globale und statische Variable, über den schnellen Datenverbindungsbus an die anderen Rechnereinheiten übertragen. Die Rechnereinheiten speichern den empfangenen Status. Somit stehen jeder Rechnereinheit zu jedem Zeitpunkt sowohl die Software-Programme aller Rechnereinheiten als auch die aktuelle Information über den Status dieser Programme zur Verfügung.

Auch bei Ausfall mehrerer Rechner bleibt das Gesamtsystem noch funktionsfähig, weil jede Rechnereinheit jede andere ersetzen und deren Software-Programme mit den aktuellen Variablen starten und abarbeiten kann. Sogar bei Ausfall aller Rechner bis auf einen kann der Betrieb fortgesetzt werden, weil jeder Rechner die Software und den aktuellen Status der anderen Rechner kennt und starten kann, wobei in diesem Fall jedoch die Leistungsfähigkeit des Gesamtsystems herabgesetzt sein kann.

Zur Erreichung der Redundanz müssen bei der Erfindung keine Systemkomponenten vorgehalten werden, die für den regulären, ungestörten Betrieb nicht benötigt werden; vielmehr ist jede Rechnereinheit in Betrieb, dabei jedoch so ausgelegt, daß sie die Funktion anderer Rechnereinheiten übernehmen kann. Dadurch entsteht ein erheblicher Vorteil gegenüber den bekannten Lösungen.

Vorzugsweise sind die verwendeten Rechnereinheiten im wesentlichen identisch aufgebaut, was die Beschaffung, Wartung und Pflege der Rechnereinheiten vereinfacht.

Erfindungsgemäß sind zwei bevorzugte Verfahren zur Ermittlung des Rechners, der die Aufgabe eines ausgefallenen Rechners übernehmen soll, vorgesehen. Bei einer ersten Variante sind die Regeln für die Übernahme in tabellenartiger Form im voraus festgelegt und als Datei in allen Rechnereinheiten gespeichert. Bei einer alternativen Variante ermittelt jede Rechnereinheit zyklisch ihren Auslastungsgrad und sendet diesen zu allen anderen Rechnern. Die Auslastungsgrade der einzelnen Rechnereinheiten werden verglichen, und die Rechnereinheit mit der geringsten Auslastung übernimmt die Aufgabe der ausfallenden Rechnereinheit. Der Auslastungsgrad kann entweder zyklisch ermittelt werden oder immer dann, wenn eine Störung auftritt und die Aufgaben eines Rechners von einem anderen übernommen werden müssen.

Die Software-Programme, welche ursprünglich auf einem gestörten Rechner gelaufen sind, können von einer Rechnereinheit übernommen oder auf mehrere Rechnereinheiten verteilt werden. Bei den eingesetzten Rechnern handelt es sich vorzugsweise um sogenannte Multi-Tasking-Rechner. Multi-Tasking-Rechner können gleichzeitig parallel mehrere Programme, z. B. zur Steuerung unterschiedlicher Peripheriegeräte, abarbeiten. Diese verschiedenen Programme werden bei Ausfall des Rechners zweckmäßigerweise auf mehrere der verbleibenden Rechnereinheiten verteilt, um eine möglichst gleichmäßige Auslastung des Gesamtsystems zu erreichen.

Bei einer besonders vorteilhaften Variante der Erfindung werden die Software-Programme aller Rechnereinheiten beim Systemstart jeweils in den Arbeitsspeicher der anderen Rechnereinheiten geladen und gestartet, jedoch im Regelfall nicht aktiviert. Das heißt, daß zu

einem gegebenen Zeitpunkt immer nur eine Version jedes Software-Programms aktiv ist und somit an der Rechenverarbeitung und dem Datenverkehr teilnimmt. Bei Ausfall einer Rechnereinheit wird dann eine andere Version desselben Software-Programms, das auf dem ausgefallenen Rechner lief, aktiviert. Daraus ergibt sich eine schnellere Reaktionszeit bei Störungen von einzelnen Rechnereinheiten.

Der Datenbus zwischen den Rechnereinheiten ist vorzugsweise eine aus dem Stand der Technik an sich bekannte Hochgeschwindigkeitsdatenverbindung, womit hier Datenverbindungen mit einer Übertragungsrate von mindestens 10 Mbit/s verstanden werden sollen.

Gemäß einer besonders vorteilhaften Ausführungsform der Erfindung ist jede Rechnereinheit über einen zugeordneten Peripheriebus mit Peripheriegeräten verbunden. Sie sendet und empfängt Signale zu und von den Peripheriegeräten, die von der Software weiterverarbeitet werden. Die Vernetzung von Peripheriegeräten über Peripheriebusse ist an sich z. B. aus der Automatisierungstechnik bekannt. Erfindungsgemäß befindet sich jeweils zwischen zwei Peripheriebussen ein elektronisch steuerbarer Schalter, über den die Peripheriebusse derart miteinander verbunden werden können, daß zwei Rechnereinheiten, denen die beiden Peripheriebusse jeweils zugeordnet sind, Zugriff auf beide Peripheriebusse und die angeschlossenen Peripheriegeräte haben. Somit kann eine Rechnereinheit nicht nur die Software-Programme, einschließlich dem aktuellen Status einer anderen Rechnereinheit übernehmen, sondern auch auf deren Peripheriegeräte zugreifen.

Die vorliegende Erfindung ist besonders vorteilhaft bei solchen Fahrzeugen und Anlagen einsetzbar, welche auf eine Vielzahl von Sensoren, Aktuatoren, Anzeigen, Bedienelemente und dergleichen zugreifen und diese steuern und die besonderen Sicherheitsanforderungen unterliegen, wie militärische Landfahrzeuge. Die vorliegende Erfindung schafft eine Redundanz der Systemkomponenten, ohne einzelne Komponenten ausschließlich für den Ersatz ausgefallener Komponenten vorzuhalten. Dadurch können besonders kostengünstige Systeme entworfen werden, die genauso zuverlässig sind, wie die Systeme mit Mehrfachauslegung nach dem Stand der Technik.

Durch die offene Struktur ist das erfindungsgemäße Rechnersystem ferner leicht um zusätzliche Funktionen erweiterbar. Diese werden lediglich an den Datenbus angeschlossen, und ihre zugeordneten Peripheriebusse werden über Schalter mit den Peripheriebussen der anderen Rechnereinheiten verbunden.

Weitere Vorteile und Merkmale der vorliegenden Erfindung ergeben sich aus der folgenden detaillierten Beschreibung mit Bezug auf die Zeichnung. In den Figuren zeigen:

Fig. 1 eine schematische Darstellung eines Rechnersystems gemäß der vorliegenden Erfindung,

Fig. 2 eine schematische Darstellung einer Rechnereinheit, und

Fig. 3 eine ähnliche Ansicht wie Fig. 1, wobei jedoch eine ausgefallene Rechnereinheit gestrichelt gezeichnet ist.

Fig. 1 zeigt eine beispielhafte Ausführungsform der vorliegenden Erfindung. Diese besteht aus zwei oder mehr, bei dem gezeigten Beispiel drei Rechnereinheiten 1, 2 und 3, welche über einen schnellen Datenverbindungsbus 4, 5 und 6 miteinander verbunden sind. Der Datenverbindungsbus 4, 5, 6 kann ein ringförmiger Bus sein, auf den die jeweiligen Rechnereinheiten 1, 2 und 3 zugreifen, oder er kann, wie in Fig. 1 gezeigt, aus einzelnen Datenverbindungen 4, 5, 6 bestehen, welche jeweils zwischen zwei Rechnereinheiten bestehen.

Bei dem Datenverbindungsbus handelt es sich vorzugsweise um eine Hochgeschwindigkeitsverbindung mit einer Übertragungsrate von mindestens 10 Mbit/s.

Die Rechnereinheiten sind bei der gezeigten Ausführungsform im wesentlichen gleich aufgebaut. Eine Rechnereinheit besteht im wesentlichen aus den Baugruppen, die in Fig. 2 schematisch gezeigt sind. In einer Gehäuseeinheit 30 mit rechnerüblichen Einbauten, z. B. Netzteil und Backplane, befinden sich die Baugruppen Zentraleinheit mit Hauptspeicher und CPU 31, Massenspeicher und Controller 32, eine Schnittstellenbaugruppe 33, welche für den Anschluß an die schnelle Datenverbindung 4, 5 und 6 dient, und eine Schnittstellenbaugruppe 34, welche für den Anschluß an die Peripheriebusse 7, 8 und 9 dient.

Diese Baugruppen entsprechen dem Stand der Technik, und sie werden daher hier nicht weiter spezifiziert. Die schnellen Datenverbindungen 4, 5 und 6 bzw. der Datenverbindungsbus sind mit den nach dem Stand der Technik üblichen Mitteln aufgebaut, z. B. mit Glasfaserkabeln oder Kupferleitungen.

An jede Rechnereinheit 1, 2 und 3 ist, wie in Abb. 1 gezeigt, ein Peripheriebus 7, 8 und 9 angeschlossen, an denen wiederum Peripheriegeräte 13 bis 25 angeschlossen sind. Diese Peripheriegeräte stellen die Schnittstellen zwischen den Rechnereinheiten und der Umwelt dar, und sie umfassen Sensoren, Aktuatoren, Anzeigen, Bedienelemente, Bediengeräte und dergleichen. Die Art und Anzahl der Peripheriegeräte hängt ab von der Funktion, die von der jeweiligen Rechnereinheit in Verbindung mit den Peripheriegeräten erfüllt werden soll. Typische Bedienelemente bei Landfahrzeugen sind z. B. Lenkhändel, Gas- und Bremspedal, Richtgriff zur Steuerung von Sichtgeräten usw. Typische Aktuatoren sind Stellmotoren für die Positionierung der Sichtmittel oder zur Steuerung von Fahrfunktionen.

Die einzelnen Peripheriebusse 7, 8 und 9 sind galvanisch voneinander getrennt, sie können jedoch durch Schalterbaugruppen 10, 11 und 12, bei der gezeigten Ausführungsform paarweise, miteinander verbunden werden. Die Schalterbaugruppen enthalten steuerbare Schalter, wobei die Steuerung der Schalter über die Peripheriebusse erfolgt; d. h. jede von zwei Rechnereinheiten 1 und 2, 2 und 3, 3 und 1, deren Peripheriebusse 7 und 8, 8 und 9, 9 und 7 von einer Schalterbaugruppe 10, 11 bzw. 12 verbunden werden können, kann den entsprechenden Schalter öffnen oder schließen. Jede Schalterbaugruppe 10, 12 ist hierfür über zwei Schnittstellen an die benachbarten Peripheriebusse 7 und 8, 8 und 9, 9 und 7 angeschlossen.

Das oben beschriebene System wird erfindungsgemäß nach dem im folgenden beschriebenen Verfahren betrieben, um bei Störung oder Ausfall einer Rechnereinheit deren Funktion auf andere zu übertragen, ohne die Funktionsfähigkeit des Gesamtsystems zu beeinträchtigen.

Zunächst ist die Arbeitsweise des Rechnersystems im Normalzustand beschrieben, d. h. bei Funktionsfähigkeit aller Rechnereinheiten; dann wird das Verfahren beschrieben, das zur Anwendung kommt, wenn eine Rechnereinheit gestört ist oder ganz ausfällt.

Im Normalzustand erfüllt jeder Rechner 1, 2, 3 die ihm zugewiesene Aufgabe. Das geschieht dadurch, daß auf dem Rechner ein Software-Programm, oder eine Software, läuft, welches die Information von den Peripherie-

geräten 13 bis 25 empfängt und verarbeitet und seiner Aufgabe gemäß entsprechende Daten, Befehle und dergleichen an die Peripheriegeräte sendet. Diese Software wird in der Regel automatisch nach dem Einschalten jeder Rechnereinheit gestartet. Darüberhinaus befindet sich auf dem Massenspeicher jeder Rechnereinheit je eine Kopie der Software-Programme, welche auf den anderen Rechnereinheiten laufen. Diese Softwarekopie wird im Normalzustand nicht in den Arbeitsspeicher geladen und nicht aktiviert.

Ein wichtiges Merkmal der Erfindung ist, daß jeder Rechner zyklisch, z. B. im Abstand von wenigen Sekunden, seinen internen Status über die Hochgeschwindigkeitsdatenverbindung 4, 5 und 6 an alle anderen Rechner sendet. Der interne Status wird hier repräsentiert durch die Inhalte der in der Software vereinbarten globalen und statischen Variablen. Jede Rechnereinheit 1, 2, 3 speichert die empfangenen Daten der anderen Rechnereinheiten in seinem Speicher, z. B. dem Hauptspeicher 31 oder dem Massenspeicher 32. Ferner führt jede Rechnereinheit zyklisch einen Selbsttest durch. Das Ergebnis dieses Selbsttests wird ebenfalls über die schnelle Datenverbindung 4, 5, 6 zu den anderen Rechnern gesendet. Jeder Rechner empfängt diese Selbsttest-Meldungen der anderen Rechner und analysiert sie. Außerdem wird überprüft, ob innerhalb einer vorher vereinbarten Zeit eine Selbsttest-Meldung empfangen wird (Watchdogfunktion).

Tritt in einem Rechner eine Störung auf, die den Rechner daran hindert, seine Aufgabe korrekt auszuführen, meldet dieser seine Störung in der zyklisch gesendeten Selbsttest-Meldung. Falls der Rechner so stark gestört ist, daß er keine Meldung mehr senden kann, z. B. bei einem Totalausfall, wird von den anderen Rechnereinheiten das Ausbleiben der Meldung durch die Watchdogfunktion erkannt.

Zur Veranschaulichung ist die Ausfallsituation in Fig. 3 dargestellt. Hier wird angenommen, daß die Rechnereinheit 3 ausfällt. Sie ist daher gestrichelt gezeichnet. Sobald die anderen Rechner 1, 2 eine Störung bzw. den Ausfall des Rechners 3 erkannt haben, wird mit einem der unten näher beschriebenen Verfahren ein Rechner ermittelt, welcher die Aufgabe des ausgefallenen übernehmen soll. Dieser Rechner, z. B. Rechner 2, lädt die Kopie der Software, die auf dem ausgefallenen Rechner gelaufen ist, d. h. in diesem Fall die Kopie der Software des Rechners 3, von seinem Massenspeicher 32 in seinen Arbeitsspeicher 31 und startet sie. Durch die Verwendung eines Multi-Tasking-Betriebssystems auf allen Rechnern wird hierbei die Ausführung der bis dahin laufenden Software nicht unterbrochen. Beim Starten der neuen Software (des Rechners 3) werden die zuletzt von diesem ausgefallenen Rechner 3 gesendeten Statusdaten als Initialisierungswerte der globalen und statischen Variablen der Software verwendet. Dadurch ist der Betriebszustand der Software praktisch identisch mit dem Stand, den der ausgefallene Rechner 3 kurz vor der Störung hatte. Ferner schickt der "Ersatzrechner" 2 über seinen zugeordneten Peripheriebus 8 einen Befehl an die Schalterbaugruppe 11, um die Verbindung zwischen den Peripheriebussen 8 und 9 zu schließen. Damit hat der Rechner 2 Zugriff auf alle Peripheriegeräte 17 bis 21, die ursprünglich von dem gestörten Rechner 3 verwaltet wurden. Somit kann der Rechner 2 die Aufgabe des gestörten oder ausgefallenen Rechners ohne Einschränkung und ohne Datenverlust weiterführen.

Die Rechenleistung der Rechnereinheiten 1, 2, 3 wird beim Entwurf vorzugsweise so gewählt, daß die Mehrbelastung der CPU keine störenden Leistungsverluste verursacht. Bei einer alternativen Ausführungsform kann vorgesehen sein, die Software-Programme eines gestörten Rechners auf mehrere der ungestörten Rechner zu verteilen, so daß eine gleichmäßigere Auslastung der ungestörten Rechnereinheiten erzielt wird. Insbesondere für den Worst-Case, daß alle Rechnereinheiten bis auf eine ausfallen, ist es ferner zweckmäßig den einzelnen Software-Programmen Prioritäten zuzuweisen, so daß bei einer Überlastung der verbleibenden, ungestörten Rechnereinheit gewährleistet ist, daß die Software-Programme höchster Priorität weiterlaufen können.

Für die Ermittlung des oder der Rechner, welche die Aufgabe eines ausgefallenen Rechners übernehmen sollen, können folgende Verfahren eingesetzt werden:
Bei einer ersten Ausführungsform wird bei dem Entwurf des Systems für alle denkbaren Kombinationen von Rechnerausfällen festgelegt, welcher Rechner welche Aufgaben oder Programme übernehmen soll. Diese Festlegung kann z. B. in Form einer Tabelle dargestellt werden. In jedem Rechner ist diese Tabelle als Datei gespeichert. Bei Ausfall eines Rechners ermitteln die anderen Rechner auf der Basis dieser Tabelle, welcher Rechner die Aufgabe des ausgefallenen Rechners übernehmen soll bzw. auf welchen Rechnern welche Software-Programme des ausgefallenen Rechners gestartet werden sollen.

Gemäß einer zweiten Ausführungsform ermitteln alle Rechner laufend ihren Auslastungsgrad. Dieser wird den anderen Rechnern entweder zyklisch oder bei Bedarf, d. h. bei Auftreten einer Störung, mitgeteilt. Bei Ausfall eines Rechners übernimmt dann automatisch der Rechner mit der geringsten Auslastung dessen Aufgaben.

Das erörterte Ausführungsbeispiel der vorliegenden Erfindung bezog sich auf eine Konfiguration mit drei Rechnereinheiten und den Ausfall der Rechnereinheit 3. Das dargelegte Beispiel ist selbstverständlich übertragbar auf Systeme mit zwei, vier oder mehr Rechnern, auf den Ausfall einer beliebigen anderen Rechnereinheit sowie auf den Ausfall von mehr als einer Rechnereinheit, solange noch mindestens eine Rechnereinheit funktionsfähig ist. Es wird erwartet, daß Rechnersysteme mit 3 bis 4 Rechnereinheiten eine gute Betriebssicherheit bei vertretbarem Verwaltungsaufwand und Kosten ergeben. Auf jedem Rechner können gleichzeitig parallel mehrere Programme laufen.

Anstatt die Aufgaben eines Rechners vollständig an einen anderen Rechner zu übertragen, kann, wie gesagt, auch vorgesehen sein, dessen Aufgaben auf mehrere verbleibende Rechner zu verteilen. Die Aufgabenverteilung ist bei einer Ausführungsform im voraus in einer Tabelle festgelegt, sie kann auch gemäß eines Algorithmus ermittelt werden. Die Schalterbaugruppen 10, 11, 12 der Peripheriebusse werden so geschaltet, daß jeder Rechner, der eine Aufgabe oder Teilaufgabe des oder der ausgefallenen Rechner übernimmt, Zugriff auf deren Peripheriebusse haben.

Anstelle der ringförmigen Anordnung der Peripheriebusse 7, 8 und 9 kann z. B. auch eine sternförmige Anordnung vorgesehen werden, bei der die Peripheriebusse bei einem entsprechenden Knotenpunkt miteinander verbunden werden können.

Im folgenden ist eine vorteilhafte Modifikation des erfindungsgemäßen Verfahrens beschrieben. Bei der Übernahme der Aufgabe eines ausgefallenen Rechners durch einen anderen entsteht eine Zwischenphase, in

der die Aufgabe nicht ausgeführt wird. Diese dauert vom Ausfall des Rechners über die Erkennung des Ausfallzustands durch die anderen Rechner, das Schalten der Peripheriebusse, bis zur Beendigung des Startvorgangs der entsprechenden Software des ausgefallenen Rechners auf dem Ersatzrechner. Während sich die erste Phase bis zum Erkennen des Ausfalls in der Praxis beliebig verkürzen läßt, indem die Wiederholrate der Selbsttestmeldung erhöht sowie entsprechend die Zeitkonstante der Watchdogfunktion verringert wird, hängt die Dauer des Startvorgangs der Software von zahlreichen Parametern, wie der Komplexität der Software und der Schnelligkeit und Leistungsfähigkeit des Massenspeichers und der Zentraleinheit ab. Als eine vorteilhafte Alternative zu dem oben beschriebenen Verfahren wird daher vorgeschlagen, nach Einschalten der Rechner alle Software-Programme, die für die Ausführung der unterschiedlichen Aufgaben benötigt werden, in die Hauptspeicher alle Rechnereinheiten zu laden. Die geladenen Programme werden dann alle bis auf das, welches die ursprüngliche Aufgabe der jeweiligen Rechnereinheit durchführt, in einen passiven Zustand oder Ruhezustand versetzt. Bei Übernahme der Funktion eines ausgefallen Rechners braucht dann nur noch das entsprechende Programm mit den aktuellsten Daten initialisiert und aktiviert werden. Der langwierige Lade- und Startvorgang entfällt, und die Reaktionszeit verkürzt sich.

Bei einem Rechnersystem mit sehr vielen Rechnereinheiten kann ferner vorgesehen sein, daß nicht jede Rechnereinheit Kopien der Software-Programme aller anderen Rechnereinheiten speichert und gegebenenfalls starten kann, sondern daß vorab eine Zuordnung in Gruppen festgelegt wird, gemäß derer bestimmte Rechnereinheiten als "Ersatzrechner" für bestimmte andere Rechnereinheiten bereitgehalten werden, wodurch der Speicherbedarf in jeder Rechnereinheit herabgesetzt wird und die Verbindung der Peripheriebusse überschaubar bleibt.

Die in der vorstehenden Beschreibung, den Ansprüche und der Zeichnung offenbarten Merkmale können sowohl einzeln als auch in beliebiger Kombination wesentlich für die Verwirklichung der Erfindung sein.

Patentansprüche

1. Verfahren zum Betreiben eines Rechnersystems, welches aus wenigstens zwei Rechnereinheiten (1, 2, 3) besteht, die über einen Datenbus (4, 5, 6) miteinander verbunden sind, wobei jede Rechnereinheit einen Speicher (31, 32) hat, mit folgenden Verfahrensschritten:
   - Speichern einer Kopie der Softwareprogramme, welche auf jeder Rechnereinheit (1, 2, 3) laufen, in anderen Rechnereinheiten (1, 2, 3);
   - zyklisches Übertragen des Status der laufenden Softwareprogramme über den Datenbus (4, 5, 6) von jeder Rechnereinheit (1, 2, 3) zu den anderen Rechnereinheiten;
   - Speichern des empfangenen Status in den Rechnereinheiten (1, 2, 3); und
   - dann, wenn eine Störung in einer Rechnereinheit (3) auftritt, Starten der zugehörigen Softwareprogramme auf einer anderen Rechnereinheit (2) oder verteilt auf mehreren anderen Rechnereinheiten (1, 2) unter Verwendung des zuletzt gespeicherten Status.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß jede Rechnereinheit (1, 2, 3) zyklisch einen Selbsttest durchführt und die Ergebnisse dieses Selbsttests an die anderen Rechnereinheiten überträgt und daß dann, wenn eine Störung in einer Rechnereinheit (3) erkannt wird, oder dann, wenn nach einer vorgegebenen Zeitspanne von einer Rechnereinheit (3) kein Ergebnis übermittelt wird, die Softwareprogramme dieser einen Rechnereinheit (3) auf der (2) oder den (1, 2) anderen Rechnereinheit(en) gestartet werden.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß zu keinem Zeitpunkt mehr als eine Version eines Softwareprogrammes aktiviert wird.

4. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß die Rechnereinheiten (2; 1, 2), auf denen die Softwareprogramme der gestörten Rechnereinheit (3) gestartet werden, nach Maßgabe einer festen Zuweisung ermittelt werden.

5. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß die Rechnereinheiten (1, 2, 3) zyklisch ihre Auslastung ermitteln und den anderen Rechnereinheiten mitteilen, und daß die Rechnereinheiten (2; 1, 2), auf denen die Softwareprogramme der gestörten Rechnereinheit (3) gestartet werden, abhängig von einem Vergleich der Auslastungen der ungestörten Rechnereinheiten bestimmt werden.

6. Verfahren nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, daß
die Kopie der Softwareprogramme in einem Arbeitsspeicher (31) der Rechnereinheiten (1, 2, 3) gespeichert wird,
im ungestörten Betrieb in jeder Rechnereinheit (1, 2, 3) nur die eigene Version der Softwareprogramme aktiviert wird, und
bei Störung einer Rechnereinheit (3) die kopierte Version deren Softwareprogramme in dem Arbeitsspeicher (31) einer anderen Rechnereinheit aktiviert, mit dem zuletzt gespeicherten Status aktualisiert und gestartet wird.

7. Verfahren zum Betreiben eines Rechnersystem nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, daß die Rechnereinheiten (1, 2, 3) jeweils mit einem Peripheriebus (7, 8, 9) verbunden werden und bei Störung einer Rechnereinheit (3) deren Peripheriebus (9) mit dem Peripheriebus (7, 8) der anderen Rechnereinheit(en) (1, 2) verbunden wird.

8. Verfahren nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, daß den verschiedenen Softwareprogrammen Prioritäten zugewiesen werden, und bei Störung einer Rechnereinheit (3) die entsprechenden Softwareprogramme nach Maßgabe der Prioritäten auf der (2) oder den (1, 2) anderen Rechnereinheiten gestartet werden.

9. Rechnersystem, mit
wenigstens zwei Rechnereinheiten (1, 2, 3), einem Datenbus (4, 5, 6) zum Verbinden der Rechnereinheiten, einer Datenschnittstelle (33) in jeder Rechnereinheit zum Übertragen des Status laufender Softwareprogramme über den Datenbus (4, 5, 6) zu den jeweils anderen Rechnereinheiten (1, 2, 3),
einem Speicher (31, 32) in jeder Rechnereinheit zum Speichern einer Kopie der Softwareprogramme, welche auf den jeweils anderen Rechnereinhei-

ten (1, 2, 3) laufen, und zum Speichern des von den anderen Rechnereinheiten (1, 2, 3) übertragenen Status und
einer Steuereinrichtung (31) in jeder Rechnereinheit (1, 2, 3) zum Starten der Softwareprogramme einer anderen Rechnereinheit (3) unter Verwendung des zuletzt gespeicherten Status, wenn in dieser anderen Rechnereinheit (3) eine Störung auftritt.

10. Rechnersystem nach Anspruch 9, dadurch gekennzeichnet, daß jeder Rechnereinheit (1, 2, 3) ein Peripheriebus (7, 8, 9) zugeordnet ist, und Schaltmittel (10, 11, 12) zum wahlweisen Verbinden der Peripheriebusse (7, 8, 9) vorgesehen sind.

11. Rechnersystem nach Anspruch 10, dadurch gekennzeichnet, daß die Schaltmittel (10, 11, 12) steuerbare Schalter aufweisen.

12. Rechnersystem nach Anspruch 10 oder 11, dadurch gekennzeichnet, daß die Schaltmittel (10, 11, 12) für eine paarweise Verbindung der Peripheriebusse (7, 8, 9) angeordnet sind, so daß beide Rechnereinheiten (1, 2; 2, 3; 1, 3), die einem Peripheriebuspaar (7, 8; 8, 9; 7, 9) zugeordnet sind, bei geschlossenen Schaltmitteln Zugriff auf beide Peripheriebusse das Paares und daran angeschlossenen Peripheriegeräte (13—16, 17—21, 22—25) haben.

13. Rechnersystem nach einem der Ansprüche 9 bis 12, dadurch gekennzeichnet, daß der Datenbus ein Hochgeschwindigkeitsdatenbus ist.

14. Rechnersystem nach einem der Ansprüche 9 bis 13, dadurch gekennzeichnet, daß drei Rechnereinheiten (1, 2, 3) vorgesehen sind.

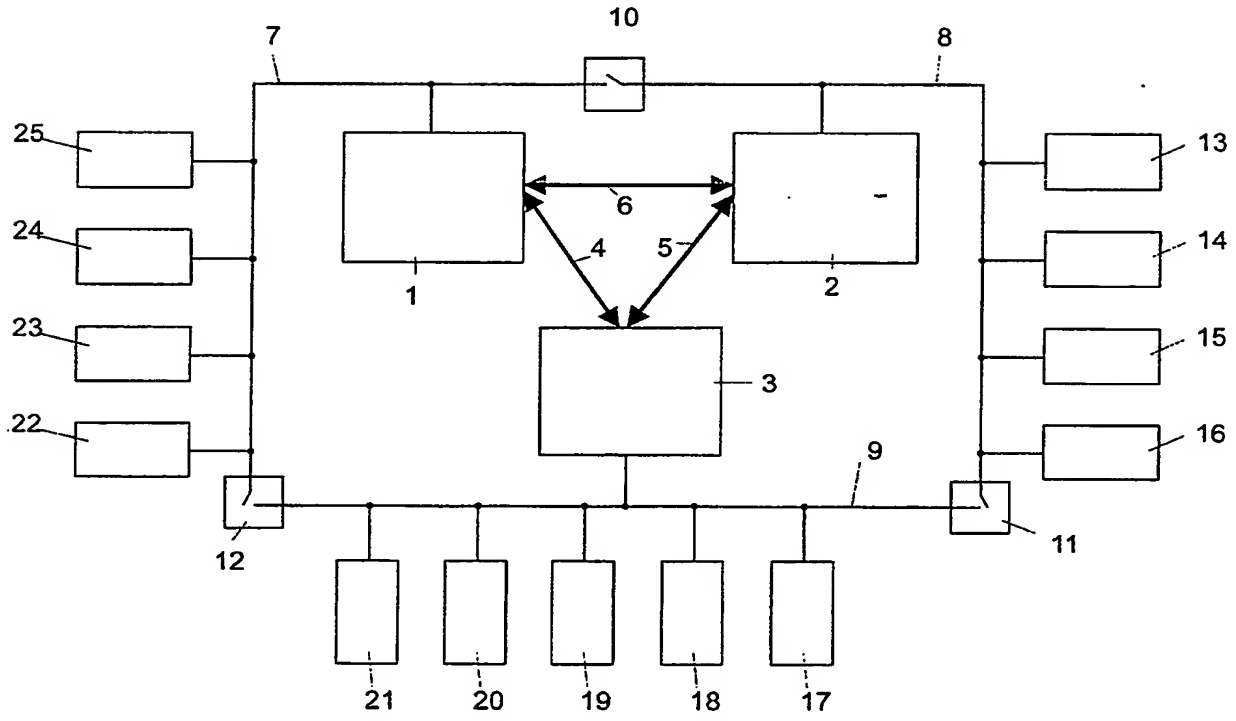
15. Rechnersystem nach Anspruch 14, dadurch gekennzeichnet, daß die Peripheriebusse (7, 8, 9) ringförmig verbunden sind.

16. Rechnersystem nach einem der Ansprüche 9 bis 15, dadurch gekennzeichnet, daß jede Rechnereinheit (1, 2, 3) einen Multitasking-Rechner aufweist.

Hierzu 2 Seite(n) Zeichnungen

Nummer: DE 196 18 105 A1
Int. Cl.[6]: G 06 F 11/20
Offenlegungstag: 13. November 1997

Fig. 1



Nummer: DE 196 18 105 A1
Int. Cl.[6]: G 06 F 11/20
Offenlegungstag: 13. November 1997

Fig. 2

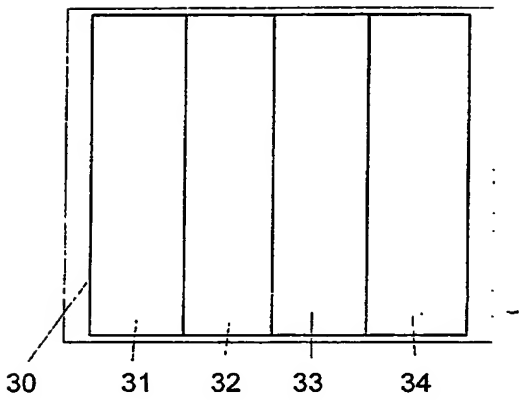


Fig. 3